

**IN THE CLAIMS**

Please substitute claims 1-42 with the following:

1. (Currently Amended) An access control system for use in a data transfer system which transfers data by means of public-key cryptosystem based on a public key certificate issued to an authentication object by a public key issuer authority, the access control system comprising:

a service provider which is an authentication object and which provides services;

a service receiving device which also is an authentication object and which receives services provided by the service provider; and

an access control server which issues to the service receiving device an access permission which identifies a service provider an access to which by the service receiving device is permitted;

a system holder which is an organization that provides or controls contents usable by a user terminal, contents which enables provision of services, or a service distribution infrastructure;

wherein the service provider performs, based on the access permission, a decision as to whether an access request by the service receiving device is to be permitted; and

the system holder is configured to administrate the service provider and the service receiving device and to treat the service provider and the service receiving device as authentication objects and generates the access permissions in a form independently usable for the service provider.

2. (Original) An access control system according to Claim 1, further comprising:  
an access-control-server registration server,  
wherein the access-control-server registration server is configured to execute a processing for requesting the access control server to execute issuance of the access permission, upon receipt of an access permission issuance request from the service receiving device.

3. (Cancelled).

4. (Currently Amended) An access control system according to ~~Claim 3~~ Claim 1, wherein a plurality of the system holders are provided, and wherein the access control server is provided for each of the system holders and is configured to issue the access permission in regard to the services provided by the service provider administrated by the system holder.

5. (Currently Amended) An access control system according to ~~Claim 3~~ Claim 1, wherein a single access control server is provided commonly for a plurality of system holders, and is configured to issue access permissions in regard to the services provided by the service providers provider administrated by the ~~plurality of~~ system holders.

6. (Currently Amended) An access control system according to ~~Claim 3~~ Claim 1, further comprising a root registration authority which administrates the system holder, wherein the root registration authority is configured to execute, based on a request from the system holder, a processing to request the public key certificate issuer authority to issue the public key certificates of the authentication objects administrated by the root registration authority.

7. (Cancelled).

8. (Original) An access control system according to Claim 1, wherein the access control server generates the access permission in a form commonly usable for a plurality of service providers.

9. (Currently Amended) An access control system according to Claim 1, wherein the ~~access control server~~ system holder is configured to generate the access permission in a format which comprises:

- an access-control-server-set fixed field set by the access control server;
- a service-provider-set option field set by ~~each of the service providers~~ provider; and
- an electronic signature field to be performed by the access control server.

10. (Currently Amended) An access control system according to Claim 9, wherein the service-provider-set option field includes identification data which indicates for ~~each of the service receiving devices~~ device whether an access by the service receiving device is permitted, and wherein the identification data includes at least one of personal information concerning the user of the associated service receiving device, user ID, user device ID, and an access permission discrimination flag.

11. (Original) An access control system according to Claim 1, wherein the data transfer between the service provider, the service receiving device and the access control server, performed directly or indirectly through an intermediary, is executed on condition that mutual authentication has been established between the sender of the data and the receiver of the data.

12. (Original) An access control system according to Claim 1, wherein the data transfer between the service provider, the service receiving device and the access control server,

performed directly or indirectly through an intermediary, transfers the data with an electronic signature of the sender added thereto.

13. (Original) An access control system according to Claim 1, wherein the service provider is a device which provides a service.

14. (Original) An access control system according to Claim 1, wherein the access control server is configured to execute an access permission changing processing for revocation of the permission set on the access permission.

15. (Currently Amended) An access control method for use in a data transfer system which transfers data by means of public-key cryptosystem based on a public key certificate issued to an authentication object by a public key issuer authority, the access control method comprising the steps of:

receiving, at a service provider, an access permission from a service receiving device, the access permission having been issued by a service control server; ~~and~~

executing, based on the access permission, a determination as to whether access requested by the service receiving device is to be permitted; and

issuing, at an access control server, an access permission which is delivered to the service receiving device and which enables identification of the service provide an access to which is permitted by the service receiving device, wherein the access permission issuing step generates the access permissions in a form independently usable for each of the service providers.

16. (Cancelled).

17. (Original) An access control method according to Claim 15, further comprising the steps of:

receiving, at an access-control-server registration server, the access permission issuance request from the service receiving device and requesting, at the access-control-server registration server, the access control server to execute the processing for issuing an access permission.

18. (Original) An access control method according to Claim 15, wherein the access permission issuing step is executed based on an issuance request from a service provider which is under the administration of a system holder as an organization that provides or controls contents usable by a user terminal, contents which enables provision of services, or a service distribution infrastructure.

19. (Cancelled).

20. (Original) An access control method according to Claim 15, wherein the access control server generates the access permission in a form commonly usable for a plurality of service providers.

21. (Currently Amended) An access control method according to Claim 15, wherein the access permission issuing step generates the access permission of a format which comprises:

an access-control-server-set fixed field set by the access control server;

a service-provider-set option field set by each of the service providers provider; and

an electronic signature field to be performed by the access control server.

22. (Currently Amended) An access control method according to Claim 15, wherein the step executed by the service provider for determining whether the access is to be permitted is executed based on identification data which determines whether the access is to be permitted for

~~each of the service receiving devices~~ device and which is contained in the access permission, the identification data including at least one of personal information concerning the user of the associated service receiving device, user ID, user device ID, and an access permission discrimination flag.

23. (Original) An access control method according to Claim 15, wherein the data transfer between the service provider, the service receiving device and the access control server, executed directly or indirectly through an intermediary, is executed on condition that mutual authentication has been established between the sender of the data and the receiver of the data.

24. (Original) An access control method according to Claim 15, wherein the data transfer between the service provider, the service receiving device and the access control server, executed directly or indirectly through an intermediary, transfers the data with an electronic signature of the sender added thereto.

25. (Original) An access control method according to Claim 15, further comprising an access permission changing processing executed by the access control server to revoke the permission set on the access permission.

26-42. (Cancelled).